Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

BROADBAND VPN LAN INTERNET VIA WI-FI WITHOUT WI-FI ROUTER USING ANDROID MOBILE

Atvar Singh [1] | C.Er. Harisharan Aggarwal [2]

[1] Department of Electronics and Communication Engg., Guru Gobind Singh College Of Engg. & Technology, Guru kashi University, Talwandi sabo, Bathinda, Punjab, India.

[2] HOD, Department of Electronics and Communication Engg., Guru Gobind Singh College Of Engg. & Technology, Guru kashi University, Talwandi sabo, Bathinda, Punjab, India

ABSTRACT

Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN(wimax) technology to enable remote users to securely connect to a private network. Many corporations are very seriously concerned about VPN security of networks. In this regards, the VPN(wimax) modem and antenna standard was developed to the standard address the security problems, no doubts virtual private networking is famous for good security for the clients past few years. But VPN Broadband connection is a major problem not make a multiuser clients, because it is a single user. In the thesis work ,VPN(wimax) broadband internet connect through Wi-Fi on android mobile with the help of nano technology based mini adapter clients sharing a broadband LAN also we make with the help of nano adapter make a multiuser

KEYWORDS: Wimax antenna, Broadband VPN, Nano mini adapter (IEEE 802.11).

I. INTRODUCTION

A Virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network

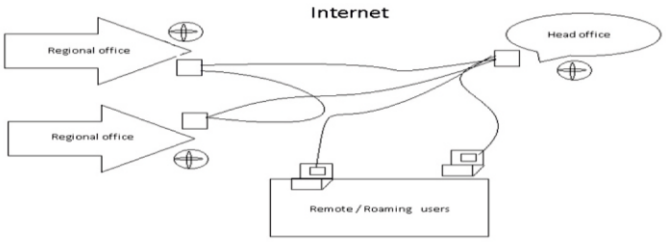

Fig 1 Internet VPN

Virtual Private Networks may allow employees to securely access a Corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their wireless transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely. Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support connect broadcast domains, so services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN). Designers have developed VPN variants, such as Virtual Private LAN Service (VPLS), and layer-2 tunneling protocols, to overcome this limitation.

II. OBJECTIVE

A virtual private network (VPN) is the essential security feature that allows remote monitoring systems to take advantage of the low communications cost of the internet. This paper introduces the VPN concept and summarizes the networking and security principles. The mechanics of security, for example, types of encryption and protocols for exchange of keys between partners, are explained. Important issues for partners in different countries include the interoperability and mutual accreditations of systems.

III. RESEARCH METHODLOGY

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys.

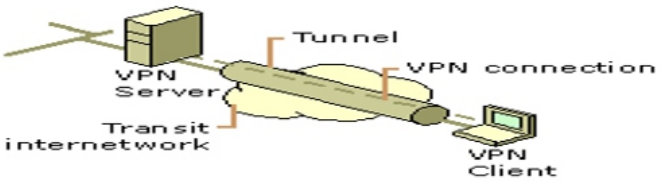

Fig 2 Virtual private network connections

VPN connections allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN connection is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

VPN technology also allows a corporation to connect to branch offices or to other companies over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites.

In both of these cases, the secure connection across the internetwork appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork—hence the name virtual private network.

VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and must be able to communicate with each other.

To provide employees with the ability to connect to corporate computing resources, regardless of their location, a corporation must deploy a scalable

remote access solution. Typically, corporations choose either an MIS department solution, where an internal information systems department is charged with buying, installing, and maintaining corporate modem pools and a private network infrastructure; or they choose a value-added network (VAN) solution, where they pay an outsourced company to buy, install, and maintain modem pools and a telecommunication infrastructure.

Neither of these solutions provides the necessary scalability, in terms of cost, flexible administration, and demand for connections. Therefore, it makes sense to replace the modem pools and private network infrastructure with a less expensive solution based on Internet technology so that the business can focus on its core competencies. With an Internet solution, a few Internet connections through Internet service providers (ISPs) and VPN server computers can serve the remote networking needs of hundreds or thousands of remote clients and branch offices.

1. **Remote Access Over the Internet VPNs** provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 2 shows a VPN connection used to connect a remote user to a corporate internet.

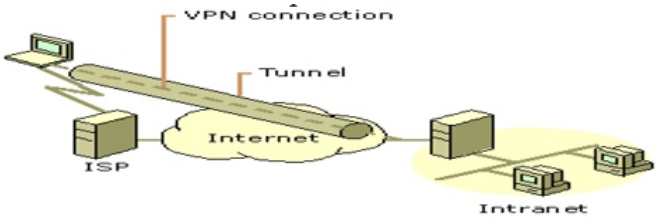

Fig 3 Using a VPN connection to connect a remote client to a private intranet

Rather than making a long distance (or 1-800) call to a corporate or outsourced network access server (NAS), the user calls a local ISP. Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

2. **Connecting Networks Over the Internet:** There are two methods for using VPNs to connect local area networks at remote sites:

- **Using dedicated lines to connect a branch office to a corporate LAN.** Rather than using an expensive long-haul dedicated circuit between the branch office and the corporate hub, both the branch office and the corporate hub routers can use a local dedicated circuit and local ISP to connect to the Internet. The VPN software uses the local ISP connections and the Internet to create a virtual private network between the branch office router and corporate hub router.

- **Using a dial-up line to connect a branch office to a corporate LAN.** Rather than having a router at the branch office make a long distance (or 1-800) call to a corporate or outsourced NAS, the router at the branch office can call the local ISP. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

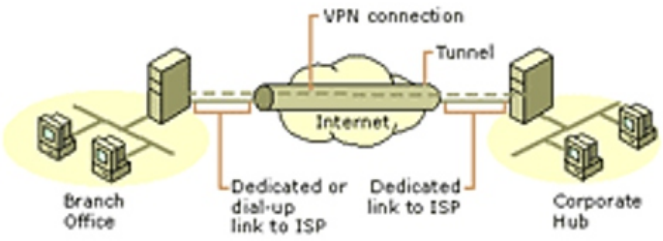

Fig 4 Using a VPN connection to connect two remote sites

In both cases, the facilities that connect the branch office and corporate offices to the Internet are local. The corporate hub router that acts as a VPN server must be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours a day for incoming VPN traffic.

Connecting Computers over an Intranet

In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork. Although this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.

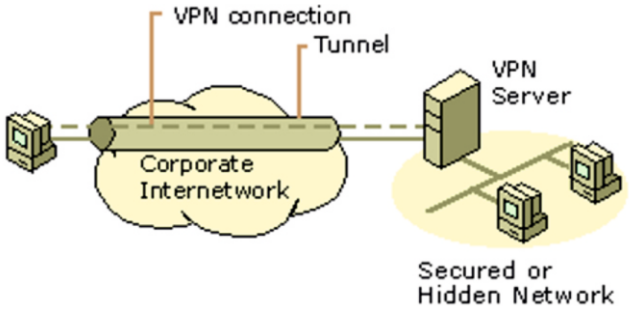

Fig 5 Using a VPN connection to connect to a secured

VPNs allow the department's LAN to be physically connected to the corporate internetwork but separated by a VPN server. The VPN server is not acting as a router between the corporate internetwork and the department LAN. A router would connect the two networks, allowing everyone access to the sensitive LAN. By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department.

IV. CONCLUSION

We lives in modern world and still many of us don't have Wi-Fi modem in our house. The reason is Wi-Fi modem/router expensive than the normal VPN- LAN and USB modem. But we do have Wi-Fi feature in our mobile phones. Many times our phones app or games requires big data to be download via 4g or Wi-Fi. 4G is still an expensive connection for average income family users and without a Wi-Fi router we can't actually create a Wi-Fi ad-hoc network. We may have internet in our house but we don't have Wi-Fi router. That time we feel upset. Sometimes at mall, school, collage or offices we gets Wi-Fi networks and we use them. That time we recognize importance of Wi-Fi to download things faster without subscribing for an internet or 3g plan for a mobile separately. As shown in fig 6 Wi-Fi working without Wi-Fi router. Technology changes within a day. You buy something and the next day you get better stuff for cheaper price. Same way there is a small and cheap Wi-Fi adapter for your pc to create Wi-Fi ad hoc without a Wi-Fi router or modem.

Fig 6 Wi-Fi working without Wi-Fi router

If you're not able to buy wireless modem than you should go for Wi-Fi adapter and create a Wi-Fi hotspot in your house. There are many mini USB Wi-Fi adapters available on online stores. But you might get cheaper if you buy from local pc market. I had seen a cheapest Wi-Fi adapter on line. You can find the best one for you and set up your home wireless network.

REFERENCES

[1] Address Allocation for Private Internets, RFC 1918, Y. Rekhter et al., February 1996

[2] E. Rosen & Y. Rekhter (March 1999). "RFC 2547 BGP/MPLS VPNs". Internet Engineering Task Force (IETF).

[3] Cisco Systems, et al. Internet working Technologies Handbook, Third Edition. Cisco Press, 2000.

[4] International Engineering Consortium. Digital Subscriber Line 2001. Intl. Engineering Consortium, 2001, p. 40.

[5] Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p. 7

[6] Lewis, Mark (2006). Comparing, designing, and deploying VPNs (1st print. ed.). Indianapolis, Ind.: Cisco Press. pp. 5–6. ISBN 1587051796

[7] Microsoft Technet. "Virtual Private Networking: An Overview".

[8] Lewis, Mark. Comparing, Designing. And Deploying VPNs. Cisco Press, 2006, p. 5

[9] TechNet Lab. "IPv6 traffic over VPN connections".

[10] Glyn M Burton: RFC 3378 EtherIP with FreeBSD, 03 February 2011

[11] "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)

[12] Soft Ether VPN: Using HTTPS Protocol to Establish VPN Tunnels

[13] "OpenConnect". Retrieved 2013-04-08. OpenConnect is a client for Cisco's AnyConnect SSL VPN OpenConnect is not officially supported by, or associated in any way with, Cisco Systems. It just happens to interoperate with their equipment..

[14] Net-security.org news: Multi-protocol SoftEther VPN becomes open source, January 2014